Real Randomness with Noise and Chaos

by Kevin Fei
working with Professor Rajarshi Roy, Professor Tom Murphy, and Joe Hart

Random numbers are instrumental to modern computing. They are used by scientists for running simulations and by cryptographers for security. Previously, we relied on "pseudo-random" number generators, where random numbers are produced from a single number, the seed. Though to most observers the numbers would be unpredictable, if you were to obtain the seed you would know all the numbers produced by the generator. If this system had been encrypting data for a company, all security would be compromised.

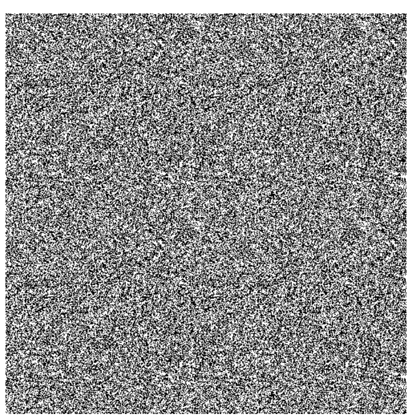
To avoid these pitfalls, we are turning to truly random physical processes to generate our numbers. These truly unpredictable processes rely on two sources of randomness: noise and chaos. Though both produce similar results, they are fundamentally different in nature. To harness them for truly random number generation, it will be critical to first understand the complex interplay between chaos and noise.

Out[1]: Click here to toggle on/off the raw code.

What is noise?

Noise refers to the random variation of values. Usually unwanted, noise causes a measurement to fluctuate over time. For example, if we're measuring the intensity of a laser, our measurement may vary over time from 900 to 881 to 913 mW. This is noise. There are many types of noise. Some of it is due to variations in the environment, like static on TV or background noise in a recording, while others are due to imperfections in the equipment like a defect in the laser.

One common method of reducing noise is to take more data. As we take more and more measurements, the final value we get will be more accurate. We are basically increasing the strength of the measurement, while the noise strength remains constant. This makes sense as flipping a coin twice cannot determine its fairness, while flipping it a hundred times will give you a better idea.

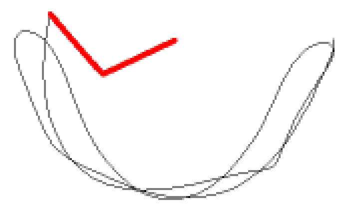


Noise in lasers

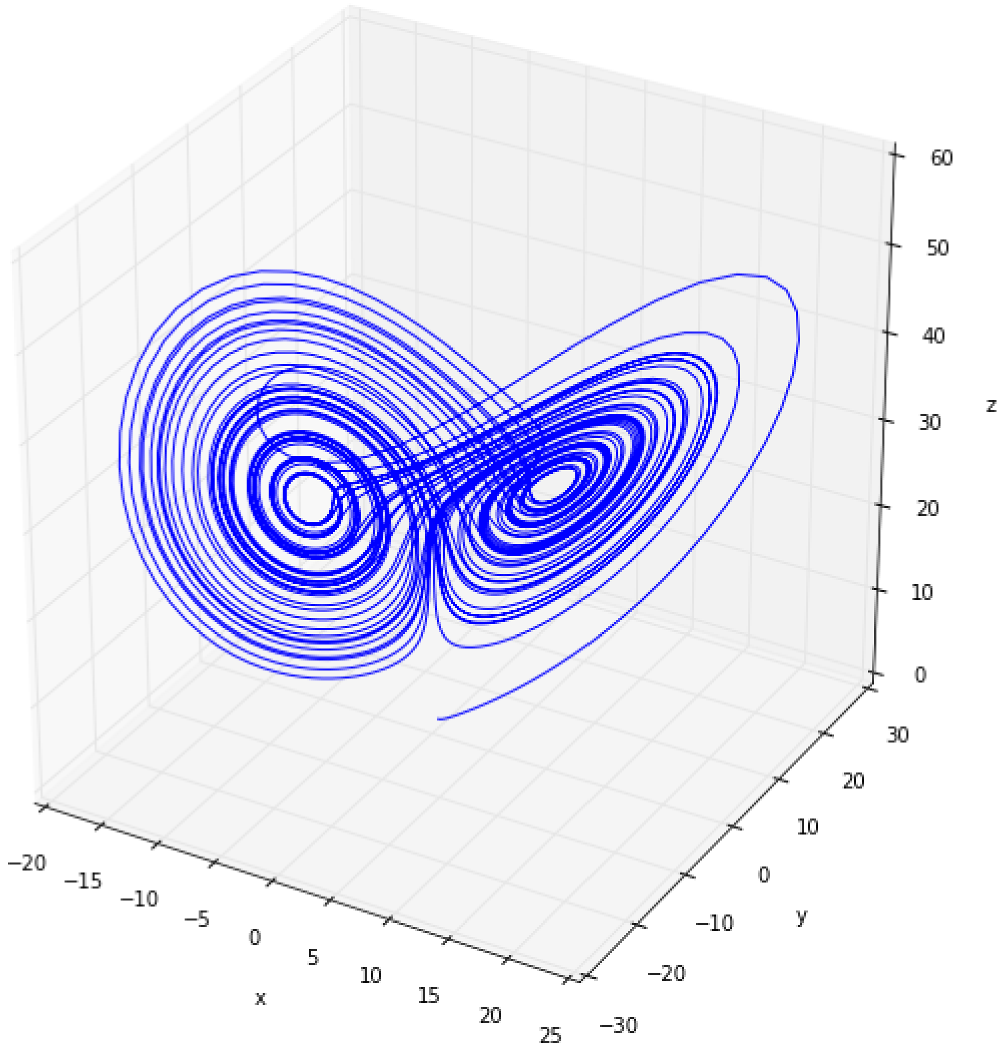
A laser works by stimulated emission, in which excited atoms release photons when other photons collide with the atoms. The first photon stimulates the second one and with this, the light intensity gets amplified. In fact, laser itself stands for Light Amplification by Stimulated Emission of Radiation. When all the light is provided by stimulated emission, all the light is synchronized and there is no noise. However, in addition to stimulated emission, lasers also randomly produce light through spontaneous emission. There is no predicting this process and thus the light intensity of the laser is noisy.

What is chaos?

Chaos happens when starting the system in a slightly different way will lead to drastially different outcomes. One example of a chaotic system is the weather. In the 1950s, mathematician Edward Lorenz attempted to model local weather based off computer simulations. He found that a tiny change in the current temperature or humidity, even dropping a decimal point off a number, could change the forecast from a sunny day to a thunderstorm. This led him to formulate the butterfly effect, noting that if a butterfly flaps their wings in Wales, it could cause a tornado in Texas. Other examples include turbulence in fluids and the double pendulum.

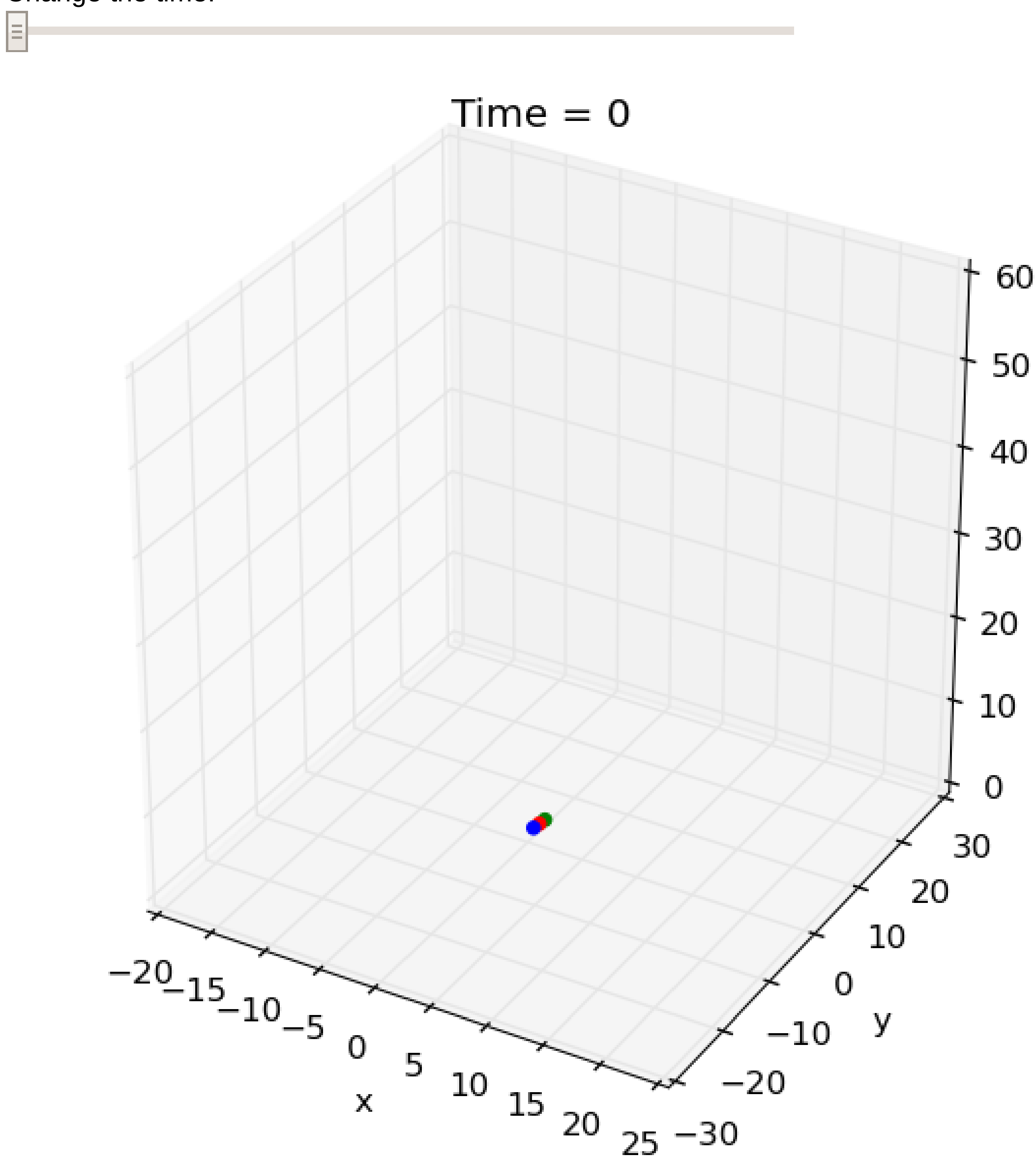


The following graph depicts the Lorenz system, a model of a point moving through space. The graph shows the path of the particle through space. The equations that control the motion are chaotic and you can see many of the characteristic features in the 3d diagram. This is called an **attractor diagram** as the path of the particle seems to be attracted to a strange butterfly shape.



As shown in the following diagram, it is apparent how quickly three points that start almost on top of each other very quickly move apart. Though the difference in initial conditions is small, their positions change in remarkably different ways. At 2 seconds, they are still close together but fly apart by 3 seconds. As time passes, the particles' movement does not show any evidence of their past similarity and it is impossible to predict where they will be.

Out[3]: Change the time:



The difference between noise and chaos

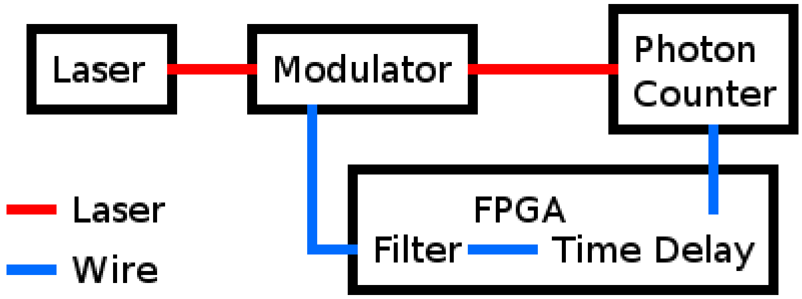
The fundamental difference between noise and chaos is that noise is **stochastic** while chaos is **deterministic**.

Stochastic means the changes in a system depend on a probability. For example, suppose you were standing on a line and flipped a coin every second. If it was heads you moved right and if it was tails you moved left. You can't predict the future because there's only a chance that you go one way or another. This property usually arises from quantum mechanics, where things are not for certain, but very likely.

Deterministic means that the system will change the same way from the same starting conditions every time. In this way one could predict the chaotic behavior if one were to know all the decimal points on a measurement. However, we cannot have perfect information (also restricted by quantum mechanics), so the tiny immeasurable differences will be amplified until the system is effectively unpredictable.

Our Experiment - The Chaotic Laser

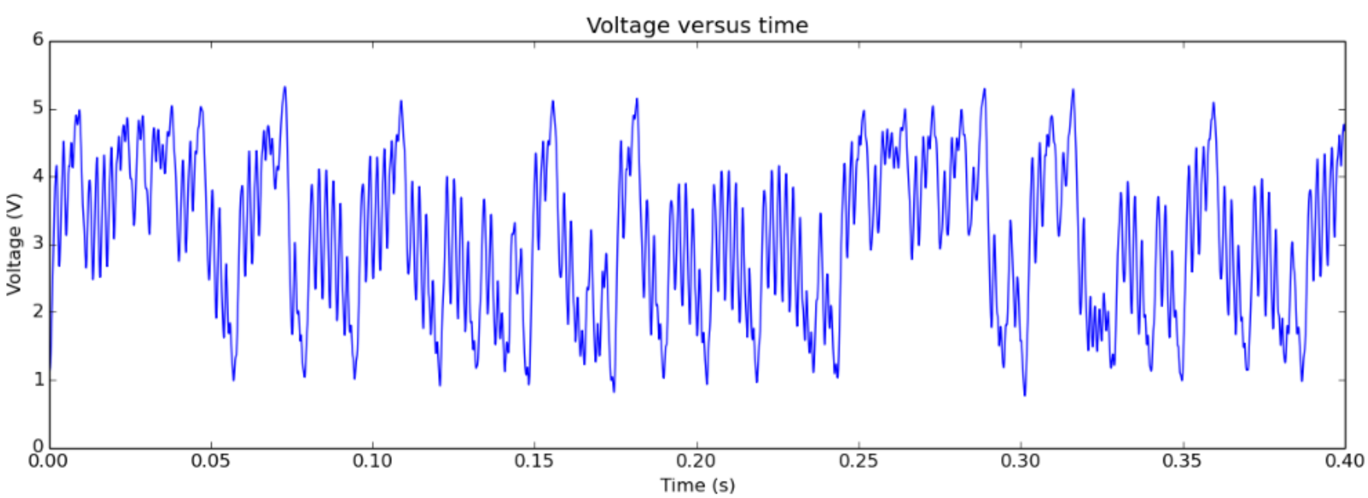
We will investigate noise and chaos in a system that contains both of these, the chaotic laser.



Let's go through the different components of the system.

- Laser - This is the driving force of the system. It shoots out a beam of light at an intensity we can control with an attenuator. This means we can change the number of photons coming out of the laser.
- Modulator - The light from the laser shines through the modulator which "modulates" or changes the intensity of light passing through it. We can change the amount it modulates by applying a voltage to it.
- Photon Counter - This instrument detects the number of photons that arrive and sends a signal to the FPGA.
- FPGA - A circuit board that contains two main important components.
  - Time Delay - Waits a certain amount of time to pass the pulses from the photon counter to the filter.
  - Filter - Applies a certain voltage to the modulator based off the arrival of photons.

In this circuit, we analyze how the voltage changes with time. We observe noise in this system with the photon counter. With more photons, we are effectively taking more measurements and lowering the amount of noise we observe. As illustrated above, the number of photons captured in a certain time interval can change randomly. Our experiment features several notable features: the *self-feedback* in the overall loop, the *nonlinearity* in the modulator, and the *time delay* in the FPGA. With our experiment configured correctly, these ingredients create chaos. This can be seen in the unpredictable voltage changing depicted below.

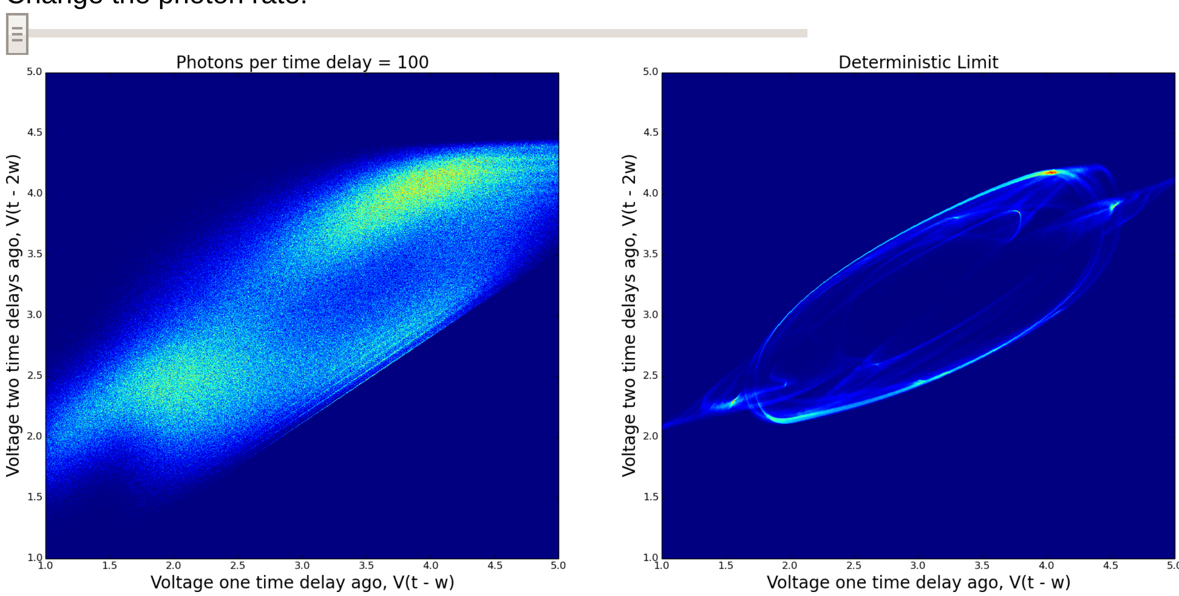


How do noise and chaos affect each other?

For a long time, scientists could not control the amount of noise in a system. It is difficult to adjust the amount of uncertainty inside a system. By adjusting the photon rate, we are in a unique position to adjust the noise level of the experiment. You can adjust the photon rate yourself with the slider! See how the graph clears up to approach the deterministic limit, explained below.

What is being graphed right here is a horizontal slice of the 3D attractor diagram (like the Lorenz diagram above). Voltage is being graphed against itself a certain time ago. With a low photon rate, an occasional spontaneous emission matters much more, making the system more noisy. This causes the diagarm to be blurred. As we turn the photon rate up, we are lowering the noise and thus we begin to see the features of the system more clearly. If we have infinite photons, we reach the **deterministic limit**, a system with no noise and pure chaos.

Out[4]: Change the photon rate:



Conclusion

Armed with the ability to vary the noise strength in our system, we can now further investigate the interplay between noise and chaos. Many have claimed that chaos, in amplifying small differences, magnifies the randomness produced by noise. This summer, our current experiment seeks to demonstrate this experimentally.